REMARKS

Applicants have thoroughly considered the Examiner's remarks in the April 24, 2008 final Office action. This Amendment D amends claims 1, 15, 22, 30, and 35. Claims 1-13, 15, 19, 20, 22, 23, 30, and 32-38 are thus presented in the application for further examination. Reconsideration of the application as amended and in view of the following remarks is respectfully requested.

Claim Rejections Under 35 U.S.C. § 103

Claims 1-13-15, 19, 20, 23, 30, 32 and 34 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Venkataramappa (U.S. Pub. App. 2003/0188193, hereinafter Venkataramappa) in view of Zhang et al. (U.S. Pat. No. 7,036,142, hereinafter Zhang) further in view of Xia et al. (U.S. Pub. No.. 2005/0005133, hereinafter Xia). Applicants respectfully disagree.

Xia teaches a method of authentication requiring a token from a management server. (Xia, Abstract). The client subsequently presents the token to a security proxy server or a host to gain access to services in accordance with the token. (Xia, Abstract). Applicants disagree with the Examiner's assertion on page 4 of the action that paragraph 36 of Xia discloses or makes obvious "storing first data on the client in response to the received first request, said first data identifying the first service wherein the authentication of the user by the first service is optional" and "allowing the user to access the first service without authenticating" as recited in claim 1.

Xia teaches **that a user is authenticated by a management server**. (FIG. 3; paragraph 33). And **in response to the authentication, the management server generates and sends a token** containing host/port designation and other authentication information **to the user**. (FIG. 3, 202-210; paragraph 34). In an embodiment, the user presents the token to the security proxy server 54 to access resources and services of the host 53. (FIG. 3; paragraph 36). The security proxy server grants access to the host based on the token. (FIG. 3, 218; paragraph 36). As an **optional layer** of security, the "**SSL server (e.g., security proxy server 54) and client** may be authenticated by its peer in the exemplary arrangement **to provide additional security above the normal** arrangement where client authentication is optional (in this case it is the user device 50 that is not trusted by the security proxy server 54)". (Paragraph 36). Additionally, Xia goes on to explain "that once the user device 50 has authenticated the security proxy server 54 and the

security proxy server 54 has authenticated the user device 50, **the security proxy server challenges the user device 50 for the authorization token."** (FIG. 3, 214; paragraph 36). **In other words, the user is required to present the token (which requires authentication by the management server) BEFORE the security proxy server grants the user access to the requested service of the host 52.**

Claim 1

In contrast, claim 1 as amended recites:

> receiving a first request from the first network server to provide the first service to the user **wherein the user is not authenticated for the first service and not authenticated for the second service when the first request is received**;
>
> storing first data on the client in response to the received first request, said first data identifying the first service wherein authentication of the user by the first service is optional **and wherein the user is not authenticated for the first service and not authenticated for the second service when the first data is stored**;
>
> allowing the user to access the first service without authenticating the user **during which the user continues to be unauthenticated for the first service and unauthenticated for the second service**;
>
> receiving a second request from the second network server to provide the second service to the user wherein the second service requires authentication of the user;
>
> allowing the user access to the second service in response to the received second request wherein the user is authenticated for the second service in response to the received second request; and
>
> wherein, in response to the authentication of the user by the second request, the user is authenticated for the first service as a result of the stored first data.

As explained above, Xia teaches that the user is first authenticated by a management server. And **in response to the authentication, the management server generates and sends a token** containing host/port designation and other authentication information **to the user**. Next, the user presents the token to **a security proxy server** to access a service of **a host**. Xia teaches that authentication by the security proxy server is optional. However, to access the service of the host, the user must be authenticated by the management server and present a valid token. This **token is used by the security proxy server in all cases to authenticate the user before allowing access to the service of the host.**

And, even if Xia discloses authentication to a client is optional, none of the cited references (Xia, Venkataramappa, Zhang and Stanko) disclose "**storing first data on the client in response to the received first request**, said first data identifying the first service wherein authentication of the user by the first service is optional **and wherein the user is not authenticated for the first service and not authenticated for the second service when the first data is stored**" and "**in response to the authentication of the user by the second request, the user is authenticated for the first service as a result of the stored first data**" as recited in the claim 1. For example, Xia may disclose that the authentication by the security proxy server is optional, but the security proxy server **only stores the token on the client of the user in response to the authentication**.

Writing for the Supreme Court, Justice Anthony Kennedy observed that a patent claim is invalid for obviousness when the invention combines familiar elements according to known methods to produce no more than predictable results. *KSR International Co. v. Teleflex, Inc.* U.S., No. 04-1350, 4/30/07. However, in this rejection, neither the **element** of **storing first data on the client in response to the received first request ... wherein the user is not authenticated for the first service and not authenticated for the second service when the first data is stored**" nor the **result** of "**in response to the authentication of the user by the second request, the user is authenticated for the first service as a result of the stored first data**" is found in the combined art.

For at least these reasons, Applicants submit that cited references, alone or in combination, do not teach or make obvious each and every element of claim 1. As such, the rejection of claim 1 under 35 U.S.C. § 103(a) should be removed. Additionally, claims 2-13 depending from claim 1 are allowable for at least the same reasons as claim 1. Claims 22 and 35 have been amended to include similar subject matter as claim 1 and are allowable for at least the same reasons as claim 1. Claims 23 and 36-38 depend from claims 22 and 35. respectively, and are allowable for at least the same reasons as claims 22 and 35

Claim 15

Claim 15, as amended, recites:

> **receiving a first request from the first network server to provide the first service to the user wherein the first service requires authentication of the user;**

authenticating the user for the first service in response to the received first request;

allowing the user access to the first service in response to the received first request;

storing first data on the client in response to allowing the user access to the first service, said first data identifying a first policy group associated with the first service, said first policy group having a shared set of business rules to restrict authentication of a user across different domains;

receiving a second request from the second network server to provide the second service to the user wherein authentication of the user by the second service is optional **and wherein the user is not authenticated for the second service**;

if the second service is associated with the first policy group identified by the stored first data, **allowing the user access to the second service in response to the received second request wherein the user is authenticated for the second service in response to the received second request;** and

if the second service is not associated with the first policy group identified by the stored first data:

updating the stored first data to identify the second service; and

allowing the unauthenticated user to access the second service during which the user continues to be unauthenticated for the second service.

For example, the user uses the browser of client computer system to navigate to Service B, which requires the user to be authenticated because it provides personalized or premium content to the user. (Page 29, paragraph 65). As a result, Service B redirects the browser to an Authentication URL of central server and the Authentication URL prompts the user for his or her credentials. (Pages 29-30, paragraph 65). The user submits his or her credentials to central server and if the submitted credentials match an entry stored in database, then central server obtains a profile associated with the submitted credentials. (Page 30, paragraph 66). **Additionally, the central server may record the policy group of Service B (Policy Group P) in a "Visited Sites" cookie on the client.** (Page 30, paragraph 66).

Thereafter, the user navigates to a first selected service, namely, Service A which belongs to the same policy group as Service B. (Page 31, paragraph 68). Within Service A, there may be web pages that the service administrator would prefer but does not require the user to be authenticated in order to grant the user access to these web pages. (Page 29, paragraph 64). Since the user has already signed in to a site within Policy Group P, namely Service B, central

server will automatically sign in the user to Service A, and an encrypted authentication ticket and profile information of the user will be communicated to Service A. (Page 29, paragraph 68).

Writing for the Supreme Court, Justice Anthony Kennedy observed that a patent claim is invalid for obviousness when the invention combines familiar elements according to known methods to produce no more than predictable results. *KSR International Co. v. Teleflex, Inc.* U.S., No. 04-1350, 4/30/07. However, in this rejection, neither the **element** of **receiving a second request from the second network server to provide the second service to the user wherein authentication of the user by the second service is optional and wherein the user is not authenticated for the second service**, nor the **result** of **if the second service is not associated with the first policy group identified by the stored first data...allowing the unauthenticated user to access the second service during which the user continues to be unauthenticated for the second service** is found in the combined art.

For at least these reasons, Applicants submit that cited references, alone or in combination, do not teach or make obvious each and every element of claim 15. As such, the rejection of claim 15 under 35 U.S.C. § 103(a) should be removed. Additionally, claims 19 and 20 depending from claim 15 are allowable for at least the same reasons as claim 15. Claim 30 has been amended to include similar subject matter as claim 15 and is allowable for at least the same reasons as claim 15. Claims 32 and 34 depend from claim 30 and are allowable for at least the same reasons as claim 30.

Claims 35 - 40 stand rejected under35 USC 103 (a) as being obvious over Venkataramappa in view of Stanko (U.S. Pub. App. 2005/0074126)) further in view of Xia. For the reasons stated above, Applicants submit that cited references, alone or in combination, do not teach or make obvious each and every element of claim 30 such as **"if the second policy group identified by the stored information identifying the second policy group associated with the second service is not the same as the first policy group identified by the stored first data, the central server is configured to update the stored first data to identify the second service in response to the received second request and the central server is configured to allow the unauthenticated user to access the second service during which the user continues to be unauthenticated for the second service."** As such, the rejection of claim 35 under 35 U.S.C. § 103(a) should be removed. Additionally, claims 36-38 depending from claim 35 are allowable for at least the same reasons as claim 35.

Conclusion

Applicants submit that the claims are allowable for at least the reasons set forth herein. Applicants thus respectfully submit that the claims as presented are in condition for allowance and respectfully request favorable reconsideration of this application.

Although the prior art made of record and not relied upon may be considered pertinent to the disclosure, none of these references anticipates or makes obvious the recited aspects of the invention. The fact that Applicants may not have specifically traversed any particular assertion by the Office should not be construed as indicating Applicants' agreement therewith.

Applicants wish to expedite prosecution of this application. If the Examiner deems the application to not be in condition for allowance, the Examiner is invited and encouraged to telephone the undersigned to discuss making an Examiner's amendment to place the application in condition for allowance.

The Commissioner is hereby authorized to charge any deficiency or overpayment of any required fee during the entire pendency of this application to Deposit Account No. 19-1345.

Respectfully submitted,

/Barbara A. Wilkey/

Barbara A. Wilkey, Reg. No. 62,986
SENNIGER POWERS LLP
100 North Broadway, 17th Floor
St. Louis, Missouri 63102
(314) 345-7000

FRA/BAW/cjl